Etiquette & Reminders

All participant microphones and cameras are automatically muted.

Q&A and chat are NOT moderated. Please be kind and courteous to one another.

Please enter questions and comments for presenters in the WebEx Q&A. Do not send questions via direct message to the host/panelists or in the chat feature.

For technical issues with WebEx, send a PRIVATE chat/message via WebEx to the Panelist “WEBEX Help” or email: 800-171comments@list.nist.gov
FAQ

Will this webinar be recorded?
Yes. The event will be recorded and posted at the event site within 10 business days.

When will slides be posted?
The slides will be posted by close of business on January 11, 2023 on the event site.

Does NIST issue CE/CPE credits?
No. NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

Where is the event site?
Critical Updates to NIST's CUI Publications: What You Need to Know

Ron Ross
ron.ross@nist.gov

Victoria Yan Pillitteri
victoria.yan@nist.gov
Agenda

NIST Special Publication (SP) 800-171 at a Glance

Change Overview: Final Public Draft SP 800-171 Revision 3 and Initial Public Draft SP 800-171A Revision 3

Looking Ahead for the CUI Series

Contact Information and Q&A

https://csrc.nist.gov/projects/protecting-CUI
### SP 800-171 at a Glance

<table>
<thead>
<tr>
<th>SECURITY REQUIREMENTS</th>
<th>NONFEDERAL SYSTEMS &amp; ORGANIZATIONS</th>
<th>PROCESSING, STORING, OR TRANSMITTING CUI</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR PROTECTING THE CONFIDENTIALITY OF CUI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Draft Rev 3**

- SECURITY REQUIREMENTS & ASSESSMENT PROCEDURES AVAILABLE FOR COMMENT

**International Use & Impact**

- SP 800-172

**New & Improved**

- SUPPLEMENTAL RESOURCES

**Assessment Procedures**

- SP 800-171A

- ENHANCED SECURITY REQUIREMENTS

- SP 800-172

- ASSESSMENT PROCEDURES FOR ENHANCED SECURITY REQUIREMENTS

- SP 800-172A
Overview: Final Public Draft SP 800-171 Rev 3

Improved Readability
Streamlined “Introduction” and “The Fundamentals” sections

Updated Security Requirements
• Added, deleted, or changed security requirements to reflect controls & families in SP 800-53 Rev 5 and moderate baseline in 800-53B
• Eliminated distinction between basic & derived requirements
• Increased specificity & grouped requirements
• Introduced organization-defined parameters (ODPs)
• Removed outdated & redundant requirements

Updated Tailoring Criteria
• Added new tailoring categories, NA and ORC
• Recategorized selected controls from SP 800-53B moderate baseline

Updated in Final Public Draft
• Reevaluated the tailoring categories/decisions to eliminate the NFO category
• Tailored out controls that may be adequately addressed by other related controls

Added Supplemental Resources
• Developed prototype CUI Overlay using tailored controls in SP 800-53 Rev 5
• Created transition mapping tables & analysis of changes between SP 800-171 Revision 2 and Revision 3
• Developed an FAQ

Updated in Final Public Draft
• Reduced the number of ODPs
Updated Security Requirements

✓ Updated security requirement structure
✓ Organization-defined parameters (ODP) included in some requirements
  • ODPs include assignment & selection operations
✓ Direct link to source SP 800-53 controls

3.13.10. Cryptographic Key Establishment and Management

REQUIREMENT: 03.13.10
Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key establishment and management].

DISCUSSION
Cryptographic key establishment and management include key generation, distribution, storage, access, rotation, and destruction. Cryptographic keys can be established and managed using either manual procedures or automated mechanisms supported by manual procedures. Organizations satisfy key establishment and management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards that specify appropriate options, levels, and parameters. This requirement is related to 03.13.11.

REFERENCES
Source Control: SC-12
Supporting Publications: FIPS 140-3 [38], SP 800-56A [73], SP 800-56B [74], SP 800-56C 1820 [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-63-3 [27]
## Updated Tailoring Criteria

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NCO</td>
<td>Not directly related to protecting the confidentiality of CUI</td>
<td>58</td>
<td>96</td>
</tr>
<tr>
<td>NFO</td>
<td>Expected to be implemented by nonfederal organizations without specification</td>
<td>61</td>
<td>0</td>
</tr>
<tr>
<td>FED</td>
<td>Primarily the responsibility of the Federal Government</td>
<td>18</td>
<td>21</td>
</tr>
<tr>
<td>CUI</td>
<td>Directly related to protecting the confidentiality of CUI</td>
<td>125</td>
<td>151</td>
</tr>
<tr>
<td>ORC</td>
<td>The outcome of the control relating to the protection of confidentiality of CUI is adequately covered by other related controls.</td>
<td>New in FPD SP 800-171 Rev 3</td>
<td>19</td>
</tr>
<tr>
<td>NA</td>
<td>Not Applicable</td>
<td>New in IDP SP 800-171 Rev 3</td>
<td>50</td>
</tr>
<tr>
<td><strong>[SP 800-53]</strong> Moderate Baseline Security Controls</td>
<td></td>
<td><strong>262</strong></td>
<td><strong>287</strong></td>
</tr>
</tbody>
</table>

- New tailoring categories, NA and ORC
- Recategorized selected controls from **SP 800-53B moderate baseline**

*Updated in Final Public Draft*
- Removed NFO tailoring criteria
- Added ORC (Addressed by “Other Related Controls”) tailoring criteria
- Overall, **fewer total** security requirements
## Updated Tailoring Criteria

<table>
<thead>
<tr>
<th>Unique Sort ID (800-53x5)</th>
<th>SP 800-53 Rev 5 Control &amp; Control Enhancement</th>
<th>Tailoring Decision</th>
<th>Unique Sort ID (FPD 800-171r)</th>
<th>SP 800-171 Rev 3 Security Requirement</th>
<th>Additional Tailoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-07-01-03</td>
<td>CM-7(1) Least Functionality</td>
<td>Periodic Review</td>
<td>CUI</td>
<td>03-04-06:</td>
<td>03-04-06: Least Functionality</td>
</tr>
<tr>
<td></td>
<td>(a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and</td>
<td></td>
<td></td>
<td></td>
<td>Removed CDP to assign frequency. Removed &quot;software&quot; Added &quot;connections.&quot;</td>
</tr>
<tr>
<td>CM-07-01-04</td>
<td></td>
<td>CUI</td>
<td>03-04-06c.</td>
<td>03-04.06c. Review the system periodically to identify unnecessary or nonsecure functions, ports, protocols, connections, and services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary or and/or nonsecure].</td>
<td></td>
<td></td>
<td></td>
<td>Removed CDP to assign &quot;functions, ports, protocols, software, and services within the system deemed to be unnecessary or and/or nonsecure&quot;</td>
</tr>
<tr>
<td>CM-07-01-05</td>
<td></td>
<td>CUI</td>
<td>03-04-06d.</td>
<td>03-04.06d. Disable or remove functions, ports, protocols, connections, and services that are unnecessary or nonsecure.</td>
<td></td>
</tr>
<tr>
<td>CM-07-02-00</td>
<td>CM-7(2) Least Functionality</td>
<td>Prevent Program Execution</td>
<td>ORC</td>
<td>—</td>
<td>Addressed by AC-03, AU-06, CM-02, CM-03, CM-05, CM-06, CM-07, CM-07[35]</td>
</tr>
<tr>
<td></td>
<td>Prevent program execution in accordance with [Selection</td>
<td>one or more]; [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM-07-02-01</td>
<td></td>
<td>ORC</td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM-07-05-00</td>
<td>CM-7(5) Least Functionality</td>
<td>Authorized Software</td>
<td>CUI</td>
<td>03-04-08:</td>
<td>03-04.08 Authorized Software - Allow by Exception</td>
</tr>
<tr>
<td></td>
<td>(a) Identify [Assignment: organization-defined software programs authorized to execute on the system].</td>
<td></td>
<td></td>
<td></td>
<td>Removed CDP to assign &quot;software programs authorized to execute on the system&quot;; no change in outcome</td>
</tr>
<tr>
<td>CM-07-05-01</td>
<td></td>
<td>CUI</td>
<td>03-04-08a.</td>
<td>03-04.08a. Identify software programs authorized to execute on the system.</td>
<td></td>
</tr>
<tr>
<td>CM-07-05-02</td>
<td></td>
<td>CUI</td>
<td>03-04-08b.</td>
<td>03-04.08b. Implement a deny-all, allow-by-exception policy for the execution of software programs on the system.</td>
<td></td>
</tr>
<tr>
<td>CM-07-05-03</td>
<td>(c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].</td>
<td>CUI</td>
<td>03-04-08c.</td>
<td>03-04.08c. Review and update the list of authorized software programs periodically.</td>
<td></td>
</tr>
<tr>
<td>CM-08-00-00</td>
<td>CM-8 System Component Inventory</td>
<td></td>
<td>CUI</td>
<td>03-04-10:</td>
<td>03-04.10 System Component Inventory</td>
</tr>
<tr>
<td>CM-08-00-01</td>
<td>a. Develop and document an inventory of system components that:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CM-08-00-02</td>
<td>1. Accurately reflects the system;</td>
<td>CUI</td>
<td>03-04-10a.</td>
<td>03-04.10a. Develop and document an inventory of system components.</td>
<td></td>
</tr>
<tr>
<td>CM-08-00-03</td>
<td>2. Includes all components within the system;</td>
<td>NCO</td>
<td>—</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Added Supplemental Resources

- FAQ
- Transition Mapping
- Tables & Change Analysis
- Prototype CUI Overlay

### Added Supplemental Resources

#### Change Analysis SP 800-171 Rev 2 to FPD Rev 3

<table>
<thead>
<tr>
<th>Access Control</th>
<th>R2-03-04-01</th>
<th>9.1.1</th>
<th>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</th>
<th>Basic</th>
<th>R2-03-01-01</th>
<th>09:01:01</th>
<th>Account Management</th>
<th>Account Management: a. Define types of system accounts allowed and prohibited. b. Create, enable, modify, disable, and remove system accounts in accordance with organizational policy, procedures, processes, and criteria. c. Specify authorized user(s) of the system, group and role membership, and access authorizations (e.g., privileges). d. Authorize access to the system based on a valid access authorization and trusted system usage. e. Monitor the use of system accounts. f. Disable system accounts when: 1. The accounts have expired. 2. The accounts have been inactive for (Assignment: organization-defined time period). 3. The accounts are no longer associated with a user or individual. 4. The accounts are in violation of organizational policy, or 5. Significant risks associated with individuals are discovered. g. Notify organizational personnel or roles where: 1. Accounts are no longer required; 2. Users are terminated or transferred; and 3. System usage need-to-know changes for an individual.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>R2-03-04-02</td>
<td>9.1.1</td>
<td>Limit system access to the types of transactions and functions that authorized users are permitted to execute.</td>
<td>Basic</td>
<td>R2-03-01-02</td>
<td>08:01:02</td>
<td>Access Enforcement</td>
<td>Access Enforcement: Enforce approved authorizations for logical access to CUI and system resources.</td>
</tr>
<tr>
<td>Access Control</td>
<td>R2-03-04-03</td>
<td>9.1.3</td>
<td>Control the flow of CUI in accordance with approved authorizations.</td>
<td>Derived</td>
<td>R2-03-01-03</td>
<td>03:01:03</td>
<td>Information Flow Enforcement</td>
<td>Information Flow Enforcement: Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.</td>
</tr>
<tr>
<td>Access Control</td>
<td>R2-03-04-04</td>
<td>9.1.4</td>
<td>Separates the duties of individuals to reduce the risk of malfeasance activity without collusion.</td>
<td>Derived</td>
<td>R2-03-01-04</td>
<td>03:01:04</td>
<td>Separation of Duties</td>
<td>Separation of Duties: a. Identify the duties of individuals requiring separation. b. Define system access authorizations to support separation of duties.</td>
</tr>
</tbody>
</table>

**Filter and Sort by Column by “Type of Change”**
### Prototype CUI Overlay

<table>
<thead>
<tr>
<th>Unique Sort ID</th>
<th>Tailoring Decision</th>
<th>Unique Sort ID</th>
<th>Additional Tailoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-07-02-00</td>
<td>CM-7(2) Least Functionality</td>
<td>SP 800-53 Rev 5 Control &amp; Control Enhancement</td>
<td>ORC</td>
</tr>
<tr>
<td>CM-07-02-01</td>
<td>CM-7(2) Least Functionality</td>
<td>Prevent Program Execution</td>
<td>ORC</td>
</tr>
<tr>
<td>CM-07-05-00</td>
<td>CM-7(5) Least Functionality</td>
<td>Authorized Software</td>
<td>CUI</td>
</tr>
<tr>
<td>CM-07-05-01</td>
<td>(a) Identify</td>
<td>Assignment: organization-defined software programs authorized to execute on the system</td>
<td>CUI</td>
</tr>
<tr>
<td>CM-07-05-02</td>
<td>(b) Assign a deny-all, permit-by-exception policy</td>
<td>Assignment: organization-defined software programs on the system</td>
<td>CUI</td>
</tr>
<tr>
<td>CM-07-05-03</td>
<td>(c) Review and update the list of authorized software programs</td>
<td>Assignment: organization-defined frequency</td>
<td>CUI</td>
</tr>
<tr>
<td>CM-08-00-00</td>
<td>CM-8 System Component Inventory</td>
<td>Authorized Software</td>
<td>CUI</td>
</tr>
<tr>
<td>CM-08-00-01</td>
<td>1. Develop and document an inventory of system components that</td>
<td>Authorized Software</td>
<td>CUI</td>
</tr>
<tr>
<td>CM-08-00-02</td>
<td>2. Accurately reflects the system;</td>
<td>Authorized Software</td>
<td>NCO</td>
</tr>
<tr>
<td>CM-08-00-03</td>
<td>2. Includes all components within the system;</td>
<td>Authorized Software</td>
<td>NCO</td>
</tr>
</tbody>
</table>

- **Filter and Sort by Column**
- **Tailoring decisions at control- and requirement—item level**
Overview: Initial Public Draft SP 800-171A Rev 3

**Improved Readability**
- Updated “Introduction” and “The Fundamentals” sections
- One time version number update to align with SP 800-171 Rev 3

**Updated Assessment Procedures**
- Restructured assessment procedure syntax to align with NIST SP 800-53A Rev 5
- Includes ODPs (consistent with SP 800-171 security requirements)

**Added Supplemental Resources**
- SP 800-171A assessment procedures in spreadsheet format
3.13.10. Cryptographic Key Establishment and Management

REQUIREMENT: 03.13.10
Establish and manage cryptographic keys in the system in accordance with the following key management requirements: <Assignment: organization-defined requirements for key establishment and management>.

DISCUSSION
Cryptographic key establishment and management include key generation, distribution, storage, access, rotation, and destruction. Cryptographic keys can be established and managed using either manual procedures or automated mechanisms supported by manual procedures. Organizations satisfy key establishment and management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards that specify appropriate options, levels, and parameters. This requirement is related to 03.13.11.

REFERENCES
Source Control: SC-12
Supporting Publications: FIPS 140-3 [38], SP 800-56A [73], SP 800-56B [74], SP 800-56C 1820 [75], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-63-3 [27]
Looking Ahead for the CUI Series

**Phase 1**
- NIST issues pre-call for comments on the CUI Series
- Protecting CUI Project website redesign

**Phase 2**
- FY23 – FY24 (Q1)
  - Revise and issue initial public draft SP 800-171 Rev 3 for comment
  - Adjudicate comments, revise and issue final public draft SP 800-171 Rev 3 and draft SP 800-171A (Rev 3) for comment

**Phase 3**
- FY24 (Q2/Q3)
  - Finalize SP 800-171 Rev 3 and SP 800-171A

**Phase 4**
- FY24 – FY25
  - Stakeholder outreach and engagement

**Ongoing**
- Revise SP 800-172 and SP 800-172A; issue Rev 1 draft(s) for comment
- Finalize SP 800-172 Rev 1 and SP 800-172A Rev 1

We Are Here!
NIST seeks your feedback on all or parts of SP 800-171 Rev 3 (FPD) & SP 800-171A Rev 3 (IPD), specifically on the following topics:

- Recategorization of controls
- New tailoring criteria
- Organization-defined parameters (ODP)
- New/revised requirements
- Alignment of assessment procedures to SP 800-53A
- Use of ODP in assessment procedures

Submit your feedback to 800-171comments@list.nist.gov by January 12 26, 2024

Comments received in response to this request will be posted on the Protecting CUI project site.

Submitters’ names and affiliations (when provided) will be included, while contact information will be removed.
STAY IN TOUCH

CONTACT US

https://csrc.nist.gov/Projects/protecting-CUI

800-171comments@list.nist.gov

@NISTcyber